SAND2014-16426R

Exceptional service in the national interest

Sandia National Laboratories

Safety Case for Service Contracts

July 2014
Revision 0
GDL-168

Effective Date: mm/dd/yyyy
Review Date: mm/dd/yyyy

U.S. DEPARTMENT OF ENERGY | NNSA National Nuclear Security Administration

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. SAND NO. 2013-XXXXP

Facilities Management and Operations Center (FMOC) controlled documents are routed for review using the corporate Laboratories Electronic Signature System (LESS). After being notified that required corrections to a controlled document have been incorporated, key FMOC reviewers indicate their approval electronically using LESS. Records of approval are stored in the FMOC Document Management and Publication Team's electronic repository.

Approvers of record as of this revision are as follows:

Greg Kirsch, Requisite SME	**Date Approved: mm/dd/yyyy**
Israel Martinez, Manager	**Date Approved: mm/dd/yyyy**
Anthony Baca, Senior Manager	**Date Approved: mm/dd/yyyy**

Table of Contents

List of Figures

List of Tables

Change Log

Rev	By	Date	Type	Change Description	Pages
0	Greg Kirsch/Dave Bailey	7/17/14	New	Publish guideline.	All

1.0 Introduction

Safety cases developed for the Facilities Management and Operations Center (FMOC) are based on the requirements in MN471021, Work Planning and Control Criteria for Safe Design and Operations. The FMOC performs maintenance activities in various locations at Sandia National Laboratories, New Mexico (SNL/NM). SNL/NM consists of more than 6,000,000 square feet of buildings, structures, and site infrastructure on approximately 13,000 acres of land. The FMOC performs approximately 7500 service contract work orders a year to assist with operations and maintenance at the SNL/NM site and facilities. As part of the continual improvement process, this Safety Case will be reviewed and updated, as needed, or at a minimum every three years.

2.0 Approach

The majority of the work managed by the FMOC is typically categorized under the Industrial (Standard) Hazard Category; however, this work has the potential for accidents. Identifying hazards in the operating envelope is accomplished by the various service contractors following Specification 1065S, *Environment, Safety, and Health for Service Contracts*, and documented by the contractor in the Contract-Specific Safety Plan (CSSP). Hazards are evaluated with regard to consequences and are eliminated or addressed with appropriate engineered controls, administrative controls, and personal protective equipment (PPE). Passive engineered controls are design features of a system that do not require human intervention to mitigate a known hazard. Active engineered controls are design features of a system that require human intervention to mitigate a known hazard. The appropriate permits are obtained for each work order.

The FMOC uses a graded approach for review and approvals. The Senior Manager of the Maintenance Teams approves this Safety Case. The approval level for all work orders and purchase orders (POs) is the Sandia Delegated Representative (SDR).

The basis of the FMOC Safety Case for Service Contracts is the FMOC Safety Program and the Integrated Safety Management System (ISMS). Figure 1 shows the ISMS process and the associated work planning and control (WP&C) documents and requirements that provide a foundation for this safety case.

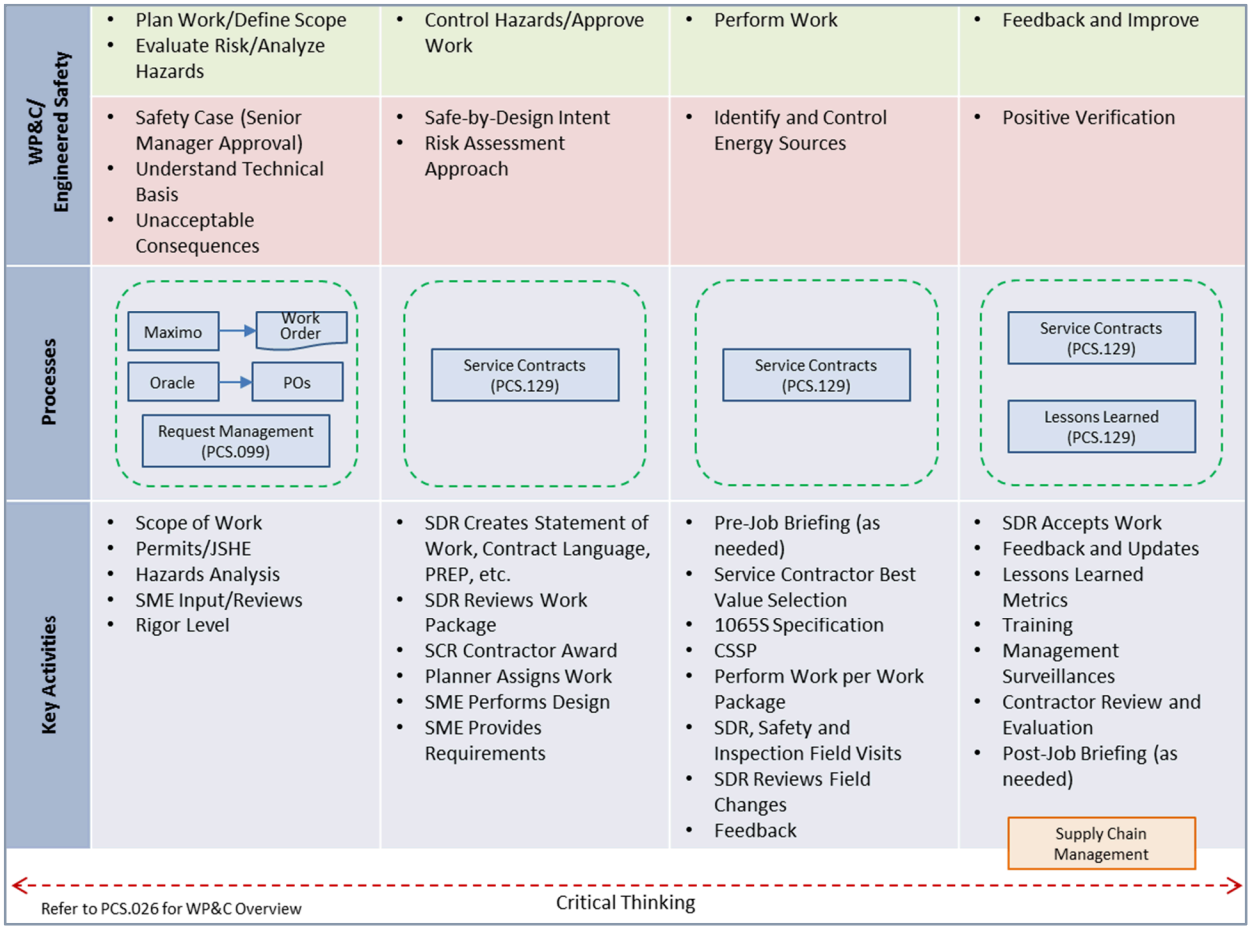

Figure 1. FMOC Service Contracts Delivery System (Engineered Safety Integration)

2.1 Safe-by-Design Intent

People tend to underestimate the probability of an accident if none have occurred previously orif the person performing the work is skilled, and they tend to trust each other's competence. Human error within systems must be identified and considered. The FMOC uses failure mode analysis (FMA) to determine how a system might fail and cause accidents, as well as the amount and types of controls needed.

The FMOC includes interconnected elements, such as people, environment, procedures, facilities, equipment, and the hazards identified in the work analysis. A daily pre-task plan is required prior to any work activity. Changes in work practices will be communicated clearly to all service contractors and personnel by way of contractor pre-task planning, activity-specific plans, contract amendments, and/or training.

The FMOC has created a safe-by-design intent approach for service contract execution starting at the planning stage and extending through the execution phase. The Safety Program(see Figure 2) summarizes how the FMOC connects work analysis elements with service contracts.

Figure 2. Safety Program

2.2 Understand the Technical Basis

The technical basis for the hazard analysis and its controls is communicated to the contractor in Specification 1065S and specified by the contractor in the CSSP.

2.3 Identify and Control Energy Sources

The FMOC service contractors address, identify, and control energy sources in all forms and, through the CSSP, work orders, and permits, manage them with appropriate engineered and administrative controls and/or PPE designed to prevent or mitigate the consequences of accidental energy releases.

2.4 Unacceptable Consequences

The JSHE and permits define the known hazards, and under Specification 1065S, workers are required to be trained to recognize abnormal, unsafe conditions and understand how to respond to the conditions by controlling and reporting the condition. Every worker understands that he/she has the responsibility and authority to suspend an activity/task if the worker believes it presents an imminent danger.

Unacceptable consequences to the FMOC include any of the following:

- Accidents that result in a serious occupational injury (per ESH100.4.RPT.3, Report Occurrences)
- Significant violation of environmental regulations
- Unplanned facility outages or interruptions that significantly impact critical mission work

2.5 Risk Assessment

The FMOC approach to risk assessment includes identifying hazards, analyzing hazards, controlling hazards, and reviewing consequences. The FMOC starts the risk assessment process in the planning stage and follows it through the work execution phase. The service contractor documents his/her hazard assessment in the CSSP. The risk assessment continues through the work execution phase by the SDR.

2.6 Positive Verification

Positive verification means that each team member must affirm to the person in charge that his or her part of the work effort is in the state intended for safe operation. Otherwise, it should be assumed by the person in charge that it is not safe to proceed. Positive verification will be implemented as part of the

service contractors' daily pre-task planning, site safety meetings, weekly progress meetings, and, as appropriate, throughout the execution of service work. In addition to contractor verification, the FMOC has safety professionals and inspection teams that conduct positive verification, including Occupational Safety and Health Administration (OSHA) compliance reviews, as part of their normal job duties.

3.0 Analyze Hazards

3.1 Detailed Identification of Hazards

The hazards are identified in the contract, scope of work, permits, JSHE, and contractor's CSSP. Hazards are broken down into two broad categories. The first category contains hazards associated with normal activities associated with the contractors' skills, with which the contractor is expected to be familiar. The second category contains hazards owned by SNL, such as laboratory equipment, chemicals, beryllium, asbestos, radioactive material, and sources. These hazards are communicated through the JSHE and permits process as shown in the work flow elements identified in Figure 3.

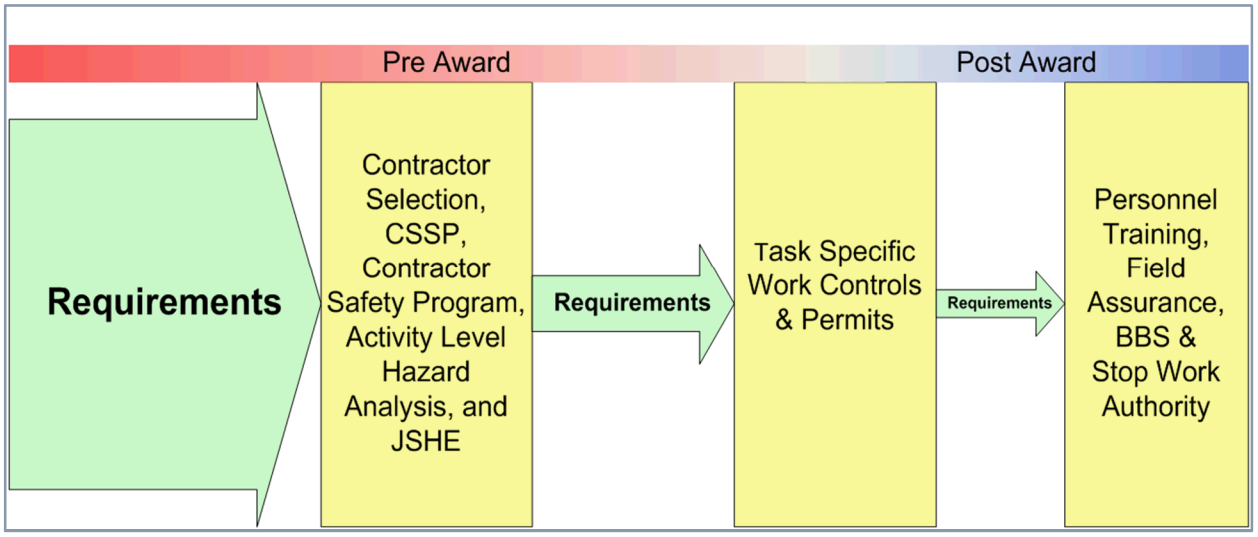

Figure 3. Work Flow Elements

3.2 Identify Safety Themes, Standards, and Codes

Once all the hazards have been identified in sufficient detail, a "safety theme" will be developed if there is a set of dominant hazards (e.g., electrical, pressure, industrial hygiene, environmental, or fire protection). A safety theme is an overarching technical strategy aimed at stimulating upfront critical thinking regarding the prevention or mitigation of accident consequences. Multiple safety themes may be necessary based on the diversity of hazards present. Use of standards and codes alone will not automatically make the work safe. If multiple hazards are present, there can be conflicts in applying standards and codes that can adversely affect the safety of the activity. The contractor's CSSP will identify safety themes. Any conflicts among standards/codes shall be resolved through the Request for Information process. If there is no dominant hazard(s), then standard service contract activity controls will be implemented.

3.3 Perform FMA

An FMA will be performed on the new or existing activities using recognized technical standards appropriate to the task. The analysis methodology selected must be capable of identifying the single-point failure modes in a system that can result in accidents with unacceptable consequences. The term "single-point failure mode" means that it only takes one failure for an accident to happen, not multiple failures. Human failure should never be automatically dismissed due to the perceived competence of team members.

The FMOC understands the unique nature of a transient work force in contracted service activities. A strong effort has been made to leverage the OSHA competent person methodology, which engages secondary analysis and permit systems for many high-risk operations.

The hazard analyses are in three different processes, which are outlined in Specification 1065S, *Environment, Safety, and Health for Service Contracts*. The FMA for construction contractors is documented in their CSSP, activity hazard analysis (AHA), and pre-task plans depending on the work. The contractor's CSSP and AHA identifies the nature of the work, the potential hazards anticipated based on the work, and how the hazards will be eliminated or mitigated. The CSSP is designed for standard industrial hazard analysis and controls. The AHA focuses on unique, nonstandard industrial hazards and controls. The pre-task plan focuses on that day's risk for specific hazards and the required critical thinking for safe operations when considering the weather, crew, and specific changes. Specific questions have been added to the pre-task plans for contractors to assist in the FMA of high-consequence operations.

4.0 Control Hazards

4.1 Eliminate Hazards and Single-Point Failures

The first priority is to eliminate the hazard rather than controlling it. The review process for the contractor's CSSP and AHA is conducted by safety professionals. This process encourages communication between work groups to help eliminate hazards and review single-point failures.

4.2 Apply Engineered and Administrative Controls

If the hazard cannot be eliminated, the hierarchy of controls is as follows:

1. Passive engineered controls
2. Active engineered controls
3. Administrative controls
4. PPE

4.3 Reviews and Approvals

This Safety Case is reviewed by the FMOC ES&H SME and the Department Manager of Service Contracts and is approved by the Senior Manager of the Maintenance Teams.

The appropriate management level will approve the work for each activity based on the hazard category shown in Table 1.

Table 1. Approval Level of the Project Execution Plan

Hazard Category	Project Execution Plan Approval
Nuclear	Vice President
Accelerator	Vice President
Industrial (High)	Vice President
Industrial (Medium)	Director
Industrial (Low)	Senior Manager
Industrial (Standard)	Manager